HERAUSGEGEBEN VON WERNER D'INKA, BERTHOLD KOHLER, GÜNTHER NONNENMACHER, FRANK SCHIRRMACHER, HOLGER STELTZNER

Frankfurter Allgemeine

Feuilleton

Ein amtlicher Trojaner

08.10.2011

Anatomie eines digitalen Ungeziefers

Wie der Staatstrojaner zerlegt wurde: Die Hacker vom Chaos Computer Club haben die Überwachungssoftware gefunden, analysiert – und gehackt. Das Ergebnis ist erschreckend. Der Trojaner kann unsere Gedanken lesen und unsere Computer fernsteuern.

Von FRANK RIEGER

Artikel

```
Dummheit ist ein grausamer, globaler Gott.
_0zapftis_aes_secretkey db 49h, 3, 93h, 8, 1
                                          ; DA
                                          ; su
    db 0A8h, 0F5h, 0Ah, 0B9h, 94h, 2, 45h,
    db 0F3h, 0ADh, 93h, 0F5h, 32h, 93h
    db    0
    db    0
    db    0
    db    0
```

© CHAOS COMPUTER CLUB

Am 27. Februar 2008 fällte das Bundesverfassungsgericht ein historisches Urteil. Als Abschluss der Auseinandersetzung um den Bundestrojaner – im Amtsdeutsch „Online-Durchsuchung“ – verkündete das höchste deutsche Gericht ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Es setzte damit sehr hohe Hürden für Geheimdienste und Ermittlungsbehörden, wenn diese die Computer von Bürgern infiltrieren wollen, um an deren digitale Lebensspuren und Daten zu gelangen. Das Urteil enthält jedoch eine Passage, die bei aufmerksamen Beobachtern schon bei der ersten Lektüre sorgenvolles Stirnrunzeln hervorrief: Es ist der Abschnitt zur sogenannten „Quellen-Telekommunikationsüberwachung“.

Die Regierung und Vertreter der Ermittlungsbehörden hatten in der Karlsruher Verhandlung vehement argumentiert, dass sie eine Möglichkeit brauchten, etwaige verschlüsselte Kommunikation schon auf dem Computer des Verdächtigen abzufangen, bevor sie verschlüsselt wird. Das Gericht mochte sich diesem Begehren nicht ganz verschließen und ließ eine sogenannte „Quellen-Telekommunikationsüberwachung“ zu – allerdings nur, „wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.“

Eingriffe von unkontrollierbarer Tiefe

Wie denn eine derartige Sicherstellung in der Praxis technisch funktionieren sollte, war schon während der mündlichen Anhörung zum Bundestrojaner in Karlsruhe ein höchst umstrittener Punkt. Das Gericht hatte die Gefahren jedenfalls erkannt und schrieb: „Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert (‚Quellen-Telekommunikationsüberwachung‘), so ist mit der Infiltration die entscheidende

Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist."

Der technische Hintergrund dieser Bedenken ist, dass ein einmal auf einem Computer installiertes Hintertürprogramm problemlos so ausgelegt werden kann, dass es Funktionen enthält oder diese über das Netz nachladen könnte, welche über das verfassungsrechtlich Zulässige weit hinausgehen. Über diese Hintertürfunktionen könnte dann unkontrollierbar tief in den geschützten Kernbereich der privaten Lebensgestaltung des Betroffenen eingegriffen werden.
Seit dem Urteil sind mehr als drei Jahre vergangen, und die deutschen Ermittlungsbehörden sind nicht untätig geblieben.

Die Ausrede liegt bereit

In Strafverfahren landauf, landab gab es in den letzten Monaten Hinweise auf den Einsatz von Trojanern zur Kommunikationsüberwachung: Wenn sich etwa Informationen in den Akten finden, die über das am Telefon Besprochene weit hinausgehen, oder Bildschirmfotos vom Rechner des Beschuldigten auftauchen, die unerklärlichen Ursprungs sind. In solchen sogenannten Screenshots werden verschiedene – in den Augen der Ermittler belastende – E-Mails oder Chat-Gespräche dokumentiert. Beantragt und richterlich genehmigt wird die sogenannte „Quellen-Telekommunikationsüberwachung" wie eine normale Telefonüberwachung. Wehren sich Beschuldigte gegen dieses Eindringen in ihre private Sphäre, reden sich die Ermittlungsbehörden damit heraus, dass die dazu eingesetzte Überwachungssoftware von einem externen, sicherheitsüberprüften Dienstleister stamme. Sie sei außerdem spezifisch entsprechend der jeweiligen Abhöranordnung zusammengestellt worden. Umfangreiche Qualitätssicherungsprozesse sollen garantieren, dass keine über die Telekommunikationsüberwachung hinausgehenden Funktionen enthalten seien. Besonders betont wird immer wieder, dass die Funktionserweiterung einer „Quellen-Telekommunikationsüberwachung" zu einer „Online-Durchsuchung" vollständig ausgeschlossen sei, mit welcher alle Daten auf einem Computer ausgespäht und alle Computerfunktionen ferngesteuert werden könnten.

Eine unabhängige technische Untersuchung dieser Angaben und Prozesse gab es bisher nicht, man musste sich auf die Beteuerungen der Behörden verlassen.
Einige der von der Spionagesoftware Betroffenen wollten nun offenbar genauer wissen, was auf ihren Computern eigentlich geschehen war und was genau alles überwacht wurde. So trafen im Verlauf der letzten Wochen diverse Festplatten in den berühmten braunen Umschlägen anonym beim Chaos Computer Club ein.
Nach kurzer forensischer Durchsicht der Datenträger durch eine Gruppe von CCC-Hackern fand sich auf einigen der Festplatten tatsächlich jeweils eine behördliche Computerwanzensoftware. Die Trojaner-Varianten sind einander ausgesprochen ähnlich und weisen nur geringfügige Unterschiede auf. Die Dateien, die einst die Betroffenen ausspioniert hatten, waren nur amateurhaft gelöscht worden und ließen sich ohne großen Aufwand mit gängigen Computerforensikwerkzeugen rekonstruieren.

Rückschlüsse auf die Funktion

Die Hacker machten sich an die Detailuntersuchung. Was sie dabei fanden, erstaunte selbst hartgesottene Zyniker. Eine Schadsoftware zu analysieren ist vergleichbar mit der Obduktion einer unbekannten Spezies von Lebewesen. Man versucht, einzelne Funktionen zu identifizieren, etwa Augen, Ohren, Atemsystem, Kreislauf, Verdauungsorgane oder Stimmapparat. Dazu zieht man Vergleiche mit bekannten Strukturen heran – etwa dass in Augen von Wirbeltieren typischerweise Linse, Hornhaut, Pupille, Glaskörper und Netzhaut zu finden sind. Aus dem Vorhandensein oder auch Fehlen dieser bekannten Strukturen erschließt man wahrscheinliche Funktionen und Zusammenhänge der Anatomie.

Mit vergleichbaren Methoden identifiziert man auch Funktionen und Zusammenhänge in einer unbekannten Schadsoftware, die ja nur als Maschinencode vorliegt. Maschinencode ist im Gegensatz zum ursprünglich in einer Programmierhochsprache wie C++ geschriebenen und später in Maschinencode übersetzten Programmcode für Menschen nur mühsam zu lesen und zu verstehen. Wenn man ergründen will, was eine

bestimmte Routine des Trojaners bewirkt, schaut man als Erstes nach, welche Funktionen des Betriebssystems sie benutzt. Das Betriebssystem eines Computers stellt ganz grundlegende Funktionen bereit, die jedes Programm benötigt, um auf dem Computer zu laufen. Dazu gehören zum Beispiel das Lesen und Schreiben von Dateien, Senden und Empfangen von Daten über das Netz, Tastatureingaben, Tonein- und -ausgabe oder auch der Start von Programmen. Einzelne Teile des Schadprogramms erfüllen verschiedene Aufgaben und benutzen also auch unterschiedliche Betriebssystemsfunktionen, aus denen sich auf ihre Funktion schließen lässt, so wie etwa ein Pathologe aus dem Vorhandensein einer Linse auf ein optisches Sinnesorgan schließen kann.

Fehlerhafte Implementierung der Verschlüsselung

Von besonderem Interesse war der bei der Analyse alsbald identifizierte Teil der Software, der für die Fernsteuerung des Trojaners über das Netz verantwortlich ist. Nach dem Start eines neu infizierten Computers bindet sich die Schadsoftware heimlich in alle laufenden Programme ein und sendet an einen fest konfigurierten Server, der sich interessanterweise in den Vereinigten Staaten – einer bekanntlich fremden Jurisdiktion – befindet, ein paar Datenpakete, um seine Dienstbereitschaft zu signalisieren. Die Pakete, die zum Server geschickt werden, sind mit einer AES-Verschlüsselung abgesichert. AES ist ein bewährtes Standardverschlüsselungsverfahren, bei dem für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Dieser Schlüssel ist in den dem CCC zugesandten Trojaner-Varianten identisch, scheint also in unterschiedlichen Überwachungsfällen wiederverwendet zu werden. Um die Kommunikation zum Server zu entschlüsseln und zu analysieren, mussten die Hacker nur den Schlüssel aus einem der Trojaner extrahieren und den Trojaner in einem von der Außenwelt isolierten Netz in Betrieb nehmen. Dabei mussten sie allerdings feststellen, dass die Verschlüsselung fachlich falsch implementiert ist, so dass auch ohne Kenntnis des Schlüssels Rückschlüsse auf den Inhalt der vom Trojaner zum Server übermittelten Daten möglich sind.

Der Trojaner sendet in regelmäßigen Abständen eine Art Parole, die benutzt wird, um dem amerikanischen Server zu signalisieren, dass es sich tatsächlich um einen von ihm kontrollierten Trojaner handelt. Die Parole der amtlichen Schadsoftware für ihren Serverzugang lautet hier C3PO-r2d2-POE. Offenbar war der Programmierer ein Star-Wars-Fan: C3PO und POE sind sogenannte Protokoll-Droiden aus dem SciFi-Universum der Star-Wars-Saga, die dort für die reibungslose Kommunikation zwischen unterschiedlichen Völkern und außerirdischen Rassen zuständig sind. Der Droide R2D2 repariert Raumschiffe.
Nachdem der Trojaner mit dieser Parole seine Anwesenheit signalisiert und noch einige weitere Daten übermittelt hat, beispielsweise eine Art digitale Fallnummer, wartet er auf Befehle vom Server. Die CCC-Hacker mussten entsetzt feststellen, dass die Schadsoftware ihre Kommandos ohne jegliche Absicherung oder Authentifizierung entgegennimmt.

Von Antivirussoftware unerkannt

Die Kommandos bestehen nur aus einzelnen Zahlen von eins bis 18 sowie einigen Parametern. Zum Absetzen der Befehle wird keine Verschlüsselung verwendet, es gibt keine kryptographische Authentifizierung oder Vergleichbares. Überall sonst im Netz, etwa beim Online-Banking oder selbst in Flirtportalen, sind das längst übliche Absicherungsmechanismen. Die einzige Bedingung für die Akzeptanz der Befehle an die staatliche Spionagesoftware aber ist es, dass sie so aussehen, als wenn sie von der IP-Adresse des Weiterleitungsservers kommen. Das Vorspiegeln einer falschen Absenderadresse ist jedoch für Kundige ein Leichtes. Dadurch hat die behördliche Computerwanze ein scheunentorgroßes Sicherheitsloch aufgestoßen, das ganz einfach ausgenutzt werden kann.

Die Funktionen, die über diese Fernsteuerungsschnittstelle aufgerufen werden können, sind aufschlussreich. Ihre Zusammenstellung und Art der Ausführung lassen keinen Zweifel daran, dass es sich um ein von Ermittlungsbehörden eingesetztes Schnüffelprogramm handelt. Die Internettelefonate mittels Skype abzuhören und Bildschirmfotos von im Vordergrund befindlichen Webbrowser-Fenstern zu machen sind genau die Funktionen, die von den Ermittlungsbehörden immer wieder lautstark

gefordert wurden, um Verschlüsselung zu umgehen, die ein „normales“ Abhören unmöglich macht. „Kommerzielle“ Trojaner, wie sie etwa zum Abschöpfen von Online-Banking-Daten verwendet werden, hätten andere, obendrein elegantere Mechanismen verwendet. Den gängigen Antivirusprogrammen ist der Trojaner völlig unbekannt.

Wege der digitalen Beweismanipulation

Die weitaus schockierendste Funktion, bei der die beteiligten Hacker zuerst ihren Augen nicht trauen wollten, wird mit dem Kommando 14 aufgerufen. Damit kann der Inhaber der Trojaner-Befehlsgewalt ein beliebiges Programm über das Netz auf den infizierten Computer laden und ausführen lassen, ohne dass der betroffene Nutzer etwas davon mitbekommt. Genau die verfassungsrechtlich höchst problematische Funktion, von der die Ermittlungsbehörden nachdrücklich behaupteten, sie sei keinesfalls in einer „Quellen-Telekommunikationsüberwachungs“-Software enthalten, fand sich bei der Analyse. Mit dem Nachladen von Programmteilen ließen sich beliebige, die Grenzen des vom Bundesverfassungsgericht Erlaubten weit überschreitende Überwachungsmodule installieren, die zum Beispiel Mikrofon und Kamera am Computer als Raumüberwachungswanze nutzen – das ist der digitale große Lausch- und Spähangriff. Genauso ist es möglich, durch dieses Programmnachladen Funktionen zu installieren, mit deren Hilfe die Festplatte des infiltrierten Computers durchsucht und Dateien heruntergeladen werden können – die exakte Definition der „Online-Durchsuchung“. Ein nachgeladenes Programm könnte sogar Dateien heimlich über das Netz auf den Computer schieben oder gespeicherte Daten verändern.

Technisch gesehen lassen sich so digitale Beweismittel problemlos erzeugen, ohne dass der Ausspionierte dies verhindern oder auch nur beweisen könnte. Finden sich auf einer Festplatte Bilder oder Filme, die Kindesmissbrauch zeigen, oder anderes schwer belastendes Material, so könnte es dort auch plaziert worden sein. Solche „Beweise“ würden zum Beispiel bei einer späteren Beschlagnahme des Computers „gefunden“ werden und sind auch mit forensischen Mitteln nicht als Fälschung erkennbar.

Mehr als nur eine Überwachung der Telekommunikation

Dass es, sobald ein Computer einmal infiltriert ist, keine Beweissicherheit mehr gibt, ist einer der gravierendsten Kritikpunkte an behördlichem Computerverseuchen überhaupt. Dass sich nun herausstellt, dass der fälschlich als „Quellen-Telekommunikationsüberwachung“ deklarierte digitale Spitzel über eine Programmnachladefunktion verfügt und obendrein diese Funktion nicht einmal rudimentär gegen einen Missbrauch durch Dritte gesichert ist, bestätigt die schlimmsten Szenarien. De facto handelt es sich hier um mehr als einen Bundestrojaner, nicht um eine begrenzte Software zum Abhören von Telekommunikation.

Alle Befürchtungen, die von Kritikern des Bundestrojaner-Einsatzes artikuliert wurden und dazu beitrugen, das Bundesverfassungsgericht zu seinem Bundestrojaner-Urteil zu veranlassen, haben sich bestätigt - manifestiert in einer Software, die eigentlich nur zur Telekommunikationsüberwachung geeignet sein soll. Mit Hilfe des Programmnachladens ist die vollständige Fernsteuerung, Manipulation und Auswertung eines infiltrierten Computers technisch möglich, auch wenn die rechtliche Ermächtigung nur für eine „Quellen-Telekommunikationsüberwachung“ galt.

Bei der detaillierten Analyse dieser Programmnachladefunktion stießen die CCC-Hacker auf ein weiteres interessantes Detail. Während der Rest der Trojaner-Software keine nennenswerten Absicherungen gegen die Erkundung seiner Funktionen durch Maschinencode-Analyse aufweist, wurde hier versucht, ausgerechnet diese heikelste Funktion abzutarnen und ihre Wirkungsweise zu verbergen.

Weiterleitungsserver im Ausland

Dazu wurden die einzelnen Softwareteile, die am Ende zur Ausführung eines über das Netz nachgeladenen Programms führen, wie Puzzlesteine verstreut, die erst dann, wenn es nötig wird, zusammengesetzt werden. Nur das zusammengesetzte Puzzle ergibt dann die Maschinencode-Routine, mit der das nachgeladene Überwachungsmodul tatsächlich in Funktion gesetzt wird. Die Auftraggeber und Programmierer des Trojaners waren sich anscheinend des massiven

verfassungsrechtlichen Verstoßes bewusst und versuchten ihr Vorgehen zu vertuschen.

Im Code des Trojaners selbst gibt es keinen Hinweis auf den Hersteller der Software. Im Jahre 2008 wurde jedoch ein interner Schriftwechsel einer Justizbehörde publik, in dem eine deutsche Firma einen Trojaner zum Skype-Abhören anbietet, deren Funktionsumfang sich mit dem von den CCC-Hackern analysierten Trojaner deckt. Sogar die Anmietung eines Weiterleitungsservers im Ausland, um die IP-Adresse der Trojaner-Kontrollstation zu verschleiern, war im Angebot erwähnt.

Zur Infiltration des Computers des Verdächtigen waren zwei Optionen aufgeführt: die Installation durch physischen Zugriff auf den Computer - vorstellbar etwa bei einem verdeckten Einbruch oder einer Personenkontrolle - und das elektronische Einschmuggeln. Letzteres erfolgt, wie aus Dokumenten zu in nordafrikanischen Diktaturen verwendeten Trojanern bekannt wurde, üblicherweise per E-Mail-Anhang oder auch durch automatisches Einfügen des Trojaners in Programme, die die Zielperson herunterlädt.

Die Überwacher schauen zu

Schon die im normalen „Lieferumfang" des Trojaners - also ohne nachgeladene Module - enthaltenen Funktionen sind geeignet, den Einsatz von staatlicher Schnüffelsoftware generell in Frage zu stellen. In schneller Folge können Bildschirmfotos von Inhalten des Webbrowsers, Chat- und E-Mail-Programmen gemacht werden, die den aktuellen Inhalt des jeweiligen Programmfensters anzeigen.

Immer mehr Menschen nutzen webbasierte Cloud-Dienste für alle wesentlichen Tätigkeiten am Computer. Egal ob Webmail-Service, Textverarbeitung und Tabellenkalkulation mit Google Docs oder Fotodienste - vieles läuft heute über den Browser. Und vom Inhalt des Browserfensters macht der Staatstrojaner auf Kommando alle paar Sekunden ein Bildschirmfoto. Die Erfassung erstreckt sich also bei weitem nicht nur auf reine Telekommunikation.

Wie bei einem Daumenkinoheftchen können die Überwacher dem Entstehen von Text gewordenen Gedanken, Kalkulationen, Notizen und E-Mails zuschauen - ein Bildschirmfoto nach dem anderen. Auch niemals versendete Nachrichten, die der Verfasser wieder gelöscht hat, statt sie abzuschicken, landen so auf dem Überwachungsserver. Viele Menschen haben es sich angewöhnt, ihre Gedanken und Gefühlen digital festzuhalten, die sie dann aber nicht unbedingt verschicken. Ohne Zweifel gehören solche intimen Notizen zum strikt geschützten Kernbereich, den das Bundesverfassungsgericht bewahrt sehen wollte. Nun landen sie mittels der Autorisierung einer einfachen Telekommunikationsüberwachung in den Handakten der Ermittler und Geheimdienste.

Überwachungsmöglichkeiten im illegalen Bereich

Um die Enttarnung von laufenden Ermittlungsmaßnahmen auszuschließen, informierte der Chaos Computer Club rechtzeitig vor der Publikation der Details des Staatstrojaners das Bundesinnenministerium. Der untersuchte staatliche Trojaner gleicht in seiner Funktion einem Parasiten, der sich im Gehirn seines Opfers einnistet, Zugriff auf seine Sinnesorgane nimmt und die Signale an seinen Herrn und Meister weiterleitet. Die Behörden haben ganz offensichtlich das in sie gesetzte Vertrauen missbraucht und heimlich genau das getan, was ihnen das Bundesverfassungsgericht untersagt hat. Die behördliche Schadsoftware ist zu einem Werkzeug geworden, das konstruiert wurde, um heimlich digitale Lebensspuren und Gedanken aus dem Computer des Verdächtigen zu extrahieren und auf Knopfdruck sogar zum großen Lausch- und Spähangriff überzugehen.

Die grundsätzliche Frage, wie viel Vertrauen Ermittlungsbehörden bei der Anwendung von neuartigen technischen Mitteln entgegengebracht werden kann, gewinnt durch die

Analyse des angeblichen „Quellen-Telekommunikationsüberwachungs“-Trojaners neue Brisanz. Es ist sicher nicht das erste Mal, dass die Polizei technische Möglichkeiten „kreativ“ genutzt hat. Es ist wohl aber das erste Mal, dass, entgegen dem expliziten Votum aus Karlsruhe, systematisch eine heimliche Ausweitung der Überwachungsmöglichkeiten in den klar illegalen Bereich vorgenommen und auch noch die Öffentlichkeit darüber irregeleitet wurde.

Wiederholte Übergriffe auf Grundrechte

Das grundlegende Vertrauen darin, dass neue Überwachungsmöglichkeiten und -befugnisse mit der von Innenpolitikern so gerne beschworenen Zurückhaltung angewendet werden, ist nachhaltig zerstört. Und wiederum erwies sich der Richtervorbehalt als zahnlos und unzureichend für den Grundrechtsschutz der Ausspionierten. Die Frage, wo die Grenzen der digitalen Intimsphäre sind, die stets zu wahren ist, stellt sich erneut dringlich.

Der Katalog der zulässigen Ermittlungsmaßnahmen und -methoden muss künftig sehr viel präziser und verbindlicher definiert werden, denn technologische Grauzonen führen immer wieder zu Grundrechtsübergriffen, die nicht sanktioniert werden. Es ist auch an der Zeit, vom Gesetzgeber ein systematisches Verwertungs- und Verwendungsverbot für rechtswidrig erlangte Beweise mit entsprechenden Sanktions- und Schadenersatzregeln einzufordern. Die Verlockung der im angelsächsischen Recht plastisch „Früchte vom verbotenen Baum“ genannten illegal beschafften Daten ist offenbar zu groß geworden.

Quelle: F.A.S.